

(REV. 12-29-99)

TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371

0655/62931

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)

09/622939

INTERNATIONAL APPLICATION NO.
PCT/IL99/00113

INTERNATIONAL FILING DATE
February 25, 1999

PRIORITY DATE CLAIMED
March 2, 1998

TITLE OF INVENTION

APPLICANT(S) FOR DO/EO/US

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
 - a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☒ has been transmitted by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ have been transmitted by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☐ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information:
 1. International Application Published Under the Patent Cooperation Treaty No. WO 99/45454 including the International Search Report
 2. Notice Informing the Applicant of the Communication of the International Application to the Designated Offices
 3. International Preliminary Examination Report

09/622959

534 Rec'd PCT/PTO 23 AUG 2000

17. ☐ The following fees are submitted:**BASIC NATIONAL FEE** (37 CFR 1.492 (a) (1) - (5)) :

Neither international preliminary examination fee (37 CFR 1.482)
nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO
and International Search Report not prepared by the EPO or JPO \$970.00

International preliminary examination fee (37 CFR 1.482) not paid to
USPTO but International Search Report prepared by the EPO or JPO \$840.00

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but
international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$690.00

International preliminary examination fee paid to USPTO (37 CFR 1.482)
but all claims did not satisfy provisions of PCT Article 33(1)-(4) \$670.00

International preliminary examination fee paid to USPTO (37 CFR 1.482)
and all claims satisfied provisions of PCT Article 33(1)-(4) \$96.00

ENTER APPROPRIATE BASIC FEE AMOUNT =

\$ 840.00

Surcharge of \$130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30
months from the earliest claimed priority date (37 CFR 1.492(e)).

\$

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE
Total claims	14 - 20 =	0	X \$18.00
Independent claims	2 - 3 =	0	X \$78.00
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ \$260.00

\$

TOTAL OF ABOVE CALCULATIONS =

\$

Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement
must also be filed (Note 37 CFR 1.9, 1.27, 1.28).

\$

SUBTOTAL =

\$

Processing fee of \$130.00 for furnishing the English translation later than ☐ 20 ☐ 30
months from the earliest claimed priority date (37 CFR 1.492(f)).

\$

TOTAL NATIONAL FEE =

\$ 840.00

Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be
accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property

\$

TOTAL FEES ENCLOSED =

\$ 840.00

Amount to be
refunded: \$
charged: \$

- a. ☒ A check in the amount of \$ 840.00 to cover the above fees is enclosed.
- b. ☐ Please charge my Deposit Account No. _____ in the amount of \$ _____ to cover the above fees.
A duplicate copy of this sheet is enclosed.
- c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any
overpayment to Deposit Account No. 03-3125. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Cooper & Dunham, LLP
1185 Avenue of the Americas
New York, N.Y. 10036



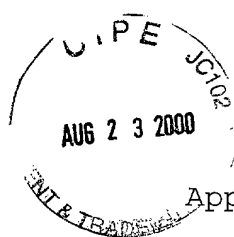
SIGNATURE:

Richard F. Jaworski

NAME

33,515

REGISTRATION NUMBER



08-24-00
422 Rec'd PCT/PTO
Dkt. 655/62931
PCT
23 AUG 2000
09/622959
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of : Doron ELGRESSY et al.

Serial No. :

Int'l Application
No.: PCT/IL99/00113

Date Filed : Concurrently Herewith

Int'l Application

Filing Date: February 25, 1999

For : METHOD AND AGENT FOR THE PROTECTION AGAINST THE
UNAUTHORIZED USE OF COMPUTER RESOURCES

1185 Avenue of the Americas
New York, N.Y. 10036

Assistant Commissioner for Patents

BOX PCT

Washington, D.C. 20231

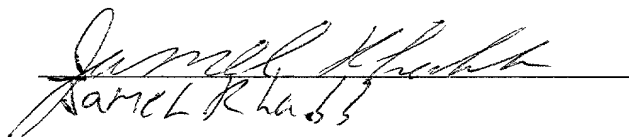
ATTN: DO/EO/US

EXPRESS MAIL
LETTER OF TRANSMITTAL

Express Mail mailing label number EM169952321US

Date of Deposit August 23, 2000

I hereby certify that the above-identified application consisting of two copies of the Transmittal Letter to the United States Designated/Elected Office (DO/EO/US) Concerning a Filing Under 35 U.S.C. 371, Information Disclosure Statement with Form PTO-1449, copy of International Application PCT/IL99/00113 filed February 25, 1999 and published September 10, 1999, copy of International Preliminary Examination Report, Preliminary Amendment and check for \$840.00 filing fee, is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.



Mail Room Employee
Depositing Express Mail Material

Attorney for Applicants:
RICHARD F. JAWORSKI, Reg. No. 33,515
Cooper & Dunham LLP
Tel: (212) 278-0400

09/622959

Dkt. 0655/62931

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



Application of: Doron ELGRESSY et al.

Serial No. :

534 Rec'd PCT/PTO 23 AUG 2000

Int'l Application

No.: PCT/IL99/00113

Date Filed : Concurrently Herewith

Int'l Application

Filing Date : February 25, 1999

For : METHOD AND AGENT FOR THE PROTECTION AGAINST THE
UNAUTHORIZED USE OF COMPUTER RESOURCES

1185 Avenue of the Americas
New York, N.Y. 10036

Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Prior to examination on the merits, please amend the claims as originally filed with the
above-identified application as follows:

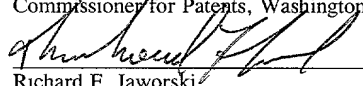
In the Claims:

Please amend claims 3, 7 and 8 as follows:

3. (Amended) A method according to claim [1 or] 2, wherein an unspecified application
is an application which is not specifically identified in a pre-set list of applications.

7. (Amended) An agent according to claim [5 or] 6, wherein said resource may be any
local or remote resource, including, but not limited to, memory allocation, files, directories,

I hereby certify that this paper is being deposited this date with the
U.S. Postal Service as first class mail addressed to Assistant
Commissioner for Patents, Washington, D.C. 20231.


Richard F. Jaworski
Reg. No. 33,515

Aug. 23, 2000
Date

operations with files and directories, such as copy, delete or compress, or any other operation leading to a permanent change in the workstation or its periphery.

8. (Amended) An agent according to [any one of claims 5 to] claim 7, further comprising a pre-set list of applications including a list of resources which each application may utilize.

Please add claims 9-14 as follows:

--9. A method according to claim 1, wherein an unspecified application is an application which is not specifically identified in a pre-set list of applications.

10. A method according to claim 9, wherein the pre-set list of applications includes a list of resources which each application may utilize.

11. An agent according to claim 5, wherein said resource may be any local or remote resource, including, but not limited to, memory allocation, files, directories, operations with files and directories, such as copy, delete or compress, or any other operation leading to a permanent change in the workstation or its periphery.

12. An agent according to claim 11, further comprising a pre-set list of applications including a list of resources which each application may utilize.

13. An agent according to claim 6, further comprising a pre-set list of applications including a list of resources which each application may utilize.

14. An agent according to claim 5, further comprising a pre-set list of applications including a list of resources which each application may utilize.--

REMARKS

Claims 3, 7 and 8 have been amended to correct formal matters and claims 9-14 have been added. Claims 1-14 are in the case, with claims 1 and 5 being in independent form.

The Office is hereby authorized to charge any additional fees which may be required in connection with this amendment and to credit any overpayment to our Deposit Account No. 03-3125.

If petition for an extension of time is required to make this response timely, this paper should be considered to be such a petition, and the Commissioner is authorized to charge the requisite fees to our Deposit Account No. 03-3125.

If a telephone interview could advance the prosecution of this application, the Examiner is respectfully requested to call the undersigned attorney.

Entry of this amendment and allowance of this application are respectfully requested.

Respectfully submitted,



RICHARD F. JAWORSKI

Reg. No.33,515

Attorney for Applicants

Cooper & Dunham LLP

Tel.: (212) 278-0400

METHOD AND AGENT FOR THE PROTECTION AGAINST THE UNAUTHORISED USE OF COMPUTER RESOURCES**Field of the Invention**

The present invention relates to the security management of computers. More particularly, the invention relates to a method and an agent for preventing the access to the use of computer resources by hostile applications.

Background of the Invention

The Internet has developed very much both in respect of its contents and of the technology employed, since it began a few years ago. In the early days of the Internet, web sites included text only, and after a while graphics was introduced. As the Internet developed, many compressed standards, such as pictures, voice and video files, were developed and with them programs used to play them (called "players"). Initially, such files were downloaded to the user's workstation only upon his request, and extracted only by the appropriate player, and after a specific order from the user.

When, in the natural course of the development of the World Wide Web the search for a way to show nicer, interactive and animated Web Pages began, Sun Microsystems Inc. developed Java - a language that allows the webmaster to write a program, a list of commands - Network Executables - that will be downloaded to the user workstation most of the time without his knowledge, and executed by his browser at his workstation. The executables are used, e.g., to provide photographic animation and other graphics on the screen of the web surfer. Such executables have ways of approaching the user

-2-

workstation's resources, which lead to a great security problem. Although some levels of security were defined in the Java language, it was very soon that a huge security hole was found in the language.

Since Java was developed, Microsoft developed ActiveX, which is another Network Executable format, also downloaded into the workstation. ActiveX has also security problems of the same kind.

The Internet has been flooded with "Network Executables" which may be downloaded -
- deliberately or without the knowledge of the users -- into workstations within organizations. These codes generally contain harmless functions. Although usually safe, they may not meet the required security policy of the organization.

Once executed, codes may jam the network, cause considerable irreversible damage to the local database, workstations and servers, or result in unauthorized retrieval of information from the servers/workstations. Such elements may appear on Java applets, ActiveX components, DLLs and other object codes, and their use is increasing at an unparalleled pace. The majority of these small programs are downloaded into the organization unsolicited and uncontrolled. The enterprise has no way of knowing about their existence or execution and there is no system in place for early detection and prevention of the codes from being executed.

The problem is made worse, in some cases, by the existence of large intranets and LANs, which may also be used by unauthorized persons to access workstations and

-3-

perform hostile activities thereon.

The security problem was solved partially by the browser manufactures which allow the user to disable the use of executables. Of course this is not a reasonable solution, since all the electronic commerce and advertising are based on the use of executables.

In three copending patent applications of the same applicants hereof, IL 120420, filed March 10, 1997, IL 121815, filed September 22, 1997, and IL 122314, filed November 27, 1997, the descriptions of which are incorporated herein by reference, there are described methods and means for preventing undesirable Executable Objects from infiltrating the LAN/WAN in which we work and, ultimately, our workstation and server. IL 122314 further provides a method for enforcing a security policy for selectively preventing the downloading and execution of undesired Executable Objects in an individual workstation.

While much has been done in the abovementioned patent applications toward protecting the individual workstation, one problem yet remained unsolved: the hostile use of local resources by applications which have passed any earlier security check (e.g., a gateway security policy), because they did not contravene such security policy, or by applications which have not passed through an earlier check point (such as a gateway equipped with a security policy check, as described in the aforementioned Israeli patent applications), either because such earlier point of check is not available, or because the application has been loaded directly on the workstation. Such hostile use of CPU resources may lead to damage to the data, operation and hardware of the workstation and, under the conditions

-4-

contemplated above, may go undetected until the damage is done.

It is an object of the present invention to provide a method and agent which overcomes the aforesaid drawbacks of prior art methods, and which provides effective protection at the workstation level.

It is another object of the present invention to provide a method and an agent which can be used effectively to prevent the hostile use of workstation resources by applications running on said workstation.

Other objects and advantages of the invention will become apparent as the description proceeds.

SUMMARY OF THE INVENTION

In one aspect, the invention is directed to a method for preventing an hostile use of computer resources by an application running on a workstation, comprising the steps of:

- a) providing a list of services that are not allowed for access by unspecified applications;
- b) when such unspecified application runs on the workstation, preventing said application from accessing any resource directly;
- c) analyzing any direct or indirect request for access to specific services, to determine whether such request is allowable according to the list defined under a) above;

-5-

- d) if the request is allowable, allowing the workstation to process it; and
- e) if the request is not allowable, preventing the unspecified application from accessing the requested resource;

wherein said resource may be any local or remote resource, including, but not limited to, memory allocation, files, directories, operations with files and directories, such as copy, delete or compress, or any other operation leading to a change in the workstation or its periphery. Illustrative - but not limitative - examples of such operations include access to system files, configuration information, network communications, hardware equipment (floppy, modem, etc.), CMOS data (time, date, etc.), or the use of resources such as memory allocation, process creation, threads creation, use of excessive CPU time, use of excessive disk space, use of excessive network communication, and use of excessive graphical resources and use of system or application configuration.

According to a preferred embodiment of the invention the list of services is provided as a look-up table.

By "unspecified application" it is meant to indicate an application that is not specifically identified in a pre-set list of applications. According to a preferred embodiment of the invention, said pre-set list of applications includes a list of resources which each application may utilize.

In another aspect, the invention is directed to an agent for protecting a workstation against the hostile use of computer resources by an unspecified application running on

-6-

said workstation, comprising:

a) means for detecting an unspecified application or a module of an application running on the workstation;

b) means for determining the requests for resources to be used by said unspecified application;

c) means for identifying chain requests for resources utilization, wherein said chain requests comprise requests made by resources called by said unspecified application;

d) means for determining whether requests made directly by said unspecified application are allowable;

e) means for determining whether requests made indirectly, as chain requests, by said unspecified application would be not allowable if made directly by said unspecified application; and

f) means for preventing said chain request from being processed, if it is determined that the request is not allowable, or that it would not be allowable if made directly by said unspecified application, and for allowing its processing if otherwise determined.

According to a preferred embodiment of the invention, the means for determining whether requests made directly or indirectly by said unspecified application are allowable comprise a look-up table including a list of services that are not allowed for access by unspecified applications. In another preferred embodiment of the invention, the agent comprises a pre-set list of applications including a list of resources that each

application may utilize.

All the above and many other characteristics and advantages of the invention, will be better understood through the following illustrative and non-limitative examples of preferred embodiments thereof, with reference to the appended drawings.

Brief Description of the Drawings

Fig. 1 schematically illustrates different applications and their requests and related operations;

Fig. 2 schematically illustrates a detail of an illustrative application that will cause machine malfunctioning; and

Fig. 3 illustrates a situation in which indirect unallowable resource exploitation is attempted.

Detailed Description of Preferred Embodiments

Examples of such situations are exemplified in Figs. 1-3. Referring to Fig. 1, three different applications are shown, marked APP1 through APP3. The process takes place at three different levels: the user mode (indicated by "U.M."), the kernel mode (indicated by "K.M."), and the hardware (indicated by "H.W."). The three different modes are schematically separated in the figure by straight lines. The APP1, APP2 and APP3 applications operate in the user mode. APP1 is an "open file" I/O request. This request is passed on to the I/O manager, which, in turn, refers to the disk(s) to perform the required operation. A filter (indicated as "S7 Filter" in the figure) analyzes the

-8-

request to determine whether it is permissible according to the security policy. If it is permissible, it is allowed to proceed to the I/O manager, which processes the request with the disk(s).

APP2, on the other hand, makes a request involving the network, i.e., and “open connection to the file server” request. The network manager is allowed to process this request only if the filter S7 has determined that it is permissible. Similarly, APP3 makes a memory allocation request, which is examined by the filter and, if permissible, is passed on to the memory manager and then acted upon in connection with the memory.

The operation of the various requests in the kernel mode and *vis-a-vis* the hardware, after the filter has examined and allowed them, is the same as with conventional operations in everyday computer, is well known to the skilled person, and therefore is not described herein in detail, for the sake of brevity.

Looking now at Fig. 2, a detail of an illustrative application that will cause machine malfunctioning is shown. In this example APP1 generates 1000 requests to generate new processes. If the system of the invention is not present, the 1000 requests will be passed on to the CPU by the Process Manager, and will use all the resources of the CPU, thus holding the work of the machine. If the filter of the invention is present, however, it may be pre-set to allow the generation of only a limited number of processes by the same application. Therefore, if a number of new processes are requested by a single application, which exceeds the preset limit, the filter S7 will not allow it to pass on to the process manager, thus avoiding the exhaustion of the resources of the machine.

Fig. 3 illustrates a situation in which indirect unallowable resources exploitation is attempted. In this example APP1 is of a type that is not allowed to send a request to the I/O Manager. If it attempts to do so, it is stopped by the S7 Filter, unless the request complies with the Security Policy preset with S7. APP1 may therefore be programmed so as to effect an interprocess communication, viz., to communicate its request to a further process, APPX, which is permitted to make the request that APP1 is not allowed to make, to the I/O Manager. In this case, the S7 filter between the User Mode and the Kernel Mode is bypassed. In order to prevent such an occurrence, a further filter S7 is located between all communicating processes, and stops any request that is passed on to one process to the other (in the example, from APP1 to APPX), and which the first process is not allowed to make directly.

Of course, as will be apparent to the skilled person, the filter S7 is not a physical filter, but rather a logical one. Logical filters of this kind can be provided in a plurality of ways, using many different analysis processes and criteria, which will be predetermined by the skilled person according to the particular requirements of the system involved.

All the above description and examples have therefore been provided for the purpose of illustration only, and are not intended to limit the invention in any way, except as defined by the appended claims.

Claims

1. A method for preventing an hostile use of computer resources by an application running on a workstation, comprising the steps of:

a) providing a list of services that are not allowed for access by unspecified applications;

b) when such unspecified application runs on the workstation, preventing said application from accessing any resource directly;

c) analyzing any direct or indirect request for access to specific services, to determine whether such request is allowable according to the list defined under a) above;

d) if the request is allowable, allowing the workstation to process it; and

e) if the request is not allowable, preventing the unspecified application from accessing the requested resource;

wherein said resource may be any local or remote resource, including, but not limited to, memory allocation, files, directories, operations with files and directories, such as copy, delete or compress, or any other operation leading to a permanent change in the workstation or its periphery.

2. A method according to claim 1, wherein the list of services is provided as a look-up table.

-11-

3. A method according to claim 1 or 2, wherein an unspecified application is an application which is not specifically identified in a pre-set list of applications.

4. A method according to claim 3, wherein the pre-set list of applications includes a list of resources which each application may utilize.

5. An agent for protecting a workstation against the hostile use of computer resources by an unspecified application running on said workstation, comprising:

a) means for detecting an unspecified application running on the workstation;

b) means for determining the requests for resources to be used by said unspecified application;

c) means for identifying chain requests for resources utilization, wherein said chain requests comprise requests made by resources called by said unspecified application;

d) means for determining whether requests made directly by said unspecified application are allowable;

e) means for determining whether requests made indirectly, as chain requests, by said unspecified application would be not allowable if made directly by said unspecified application; and

f) means for preventing said chain request from being processed, if it is determined that the request is not allowable, or that it would not be allowable if made directly by said unspecified application, and for allowing its processing if otherwise

-12-

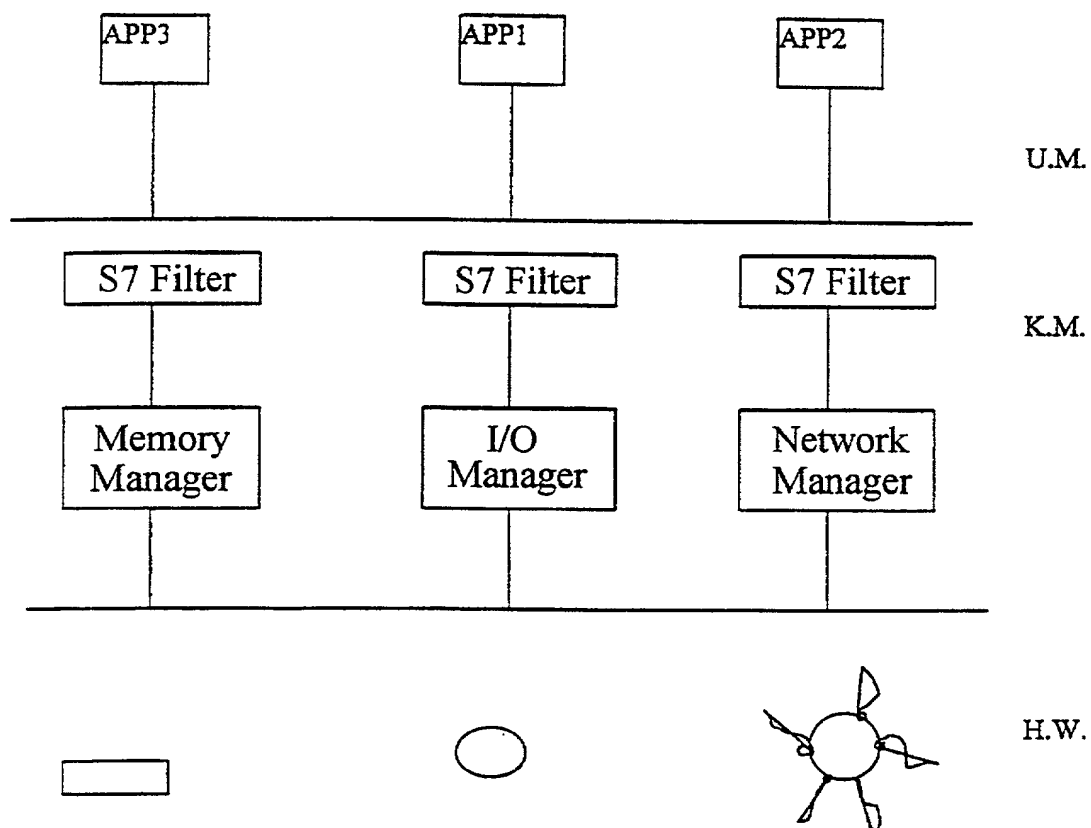
determined.

6. An agent according to claim 5, wherein the means for determining whether requests made directly or indirectly by said unspecified application are allowable comprise a look-up table including a list of services that are not allowed for access by unspecified applications.

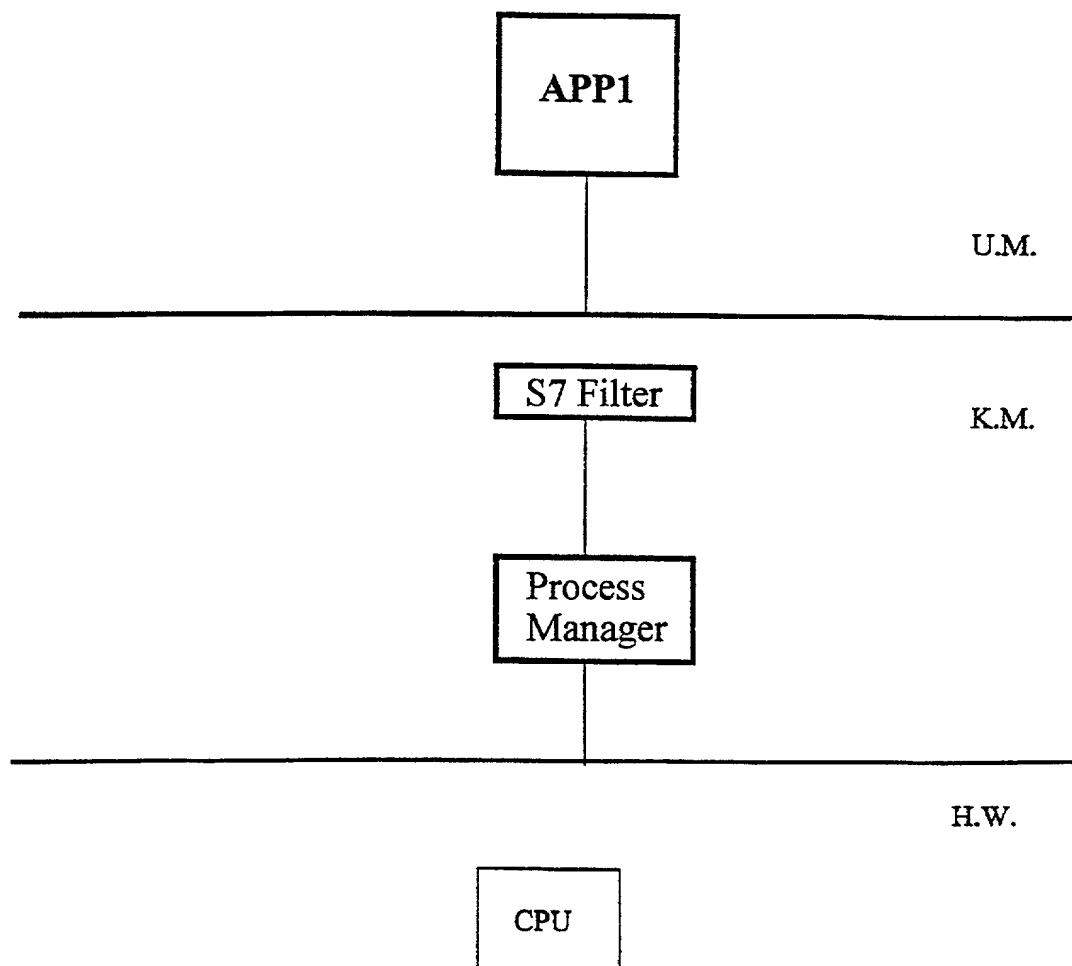
7. An agent according to claim 5 or 6, wherein said resource may be any local or remote resource, including, but not limited to, memory allocation, files, directories, operations with files and directories, such as copy, delete or compress, or any other operation leading to a permanent change in the workstation or its periphery.

8. An agent according to any one of claims 5 to 7, comprising a pre-set list of applications including a list of resources which each application may utilize.

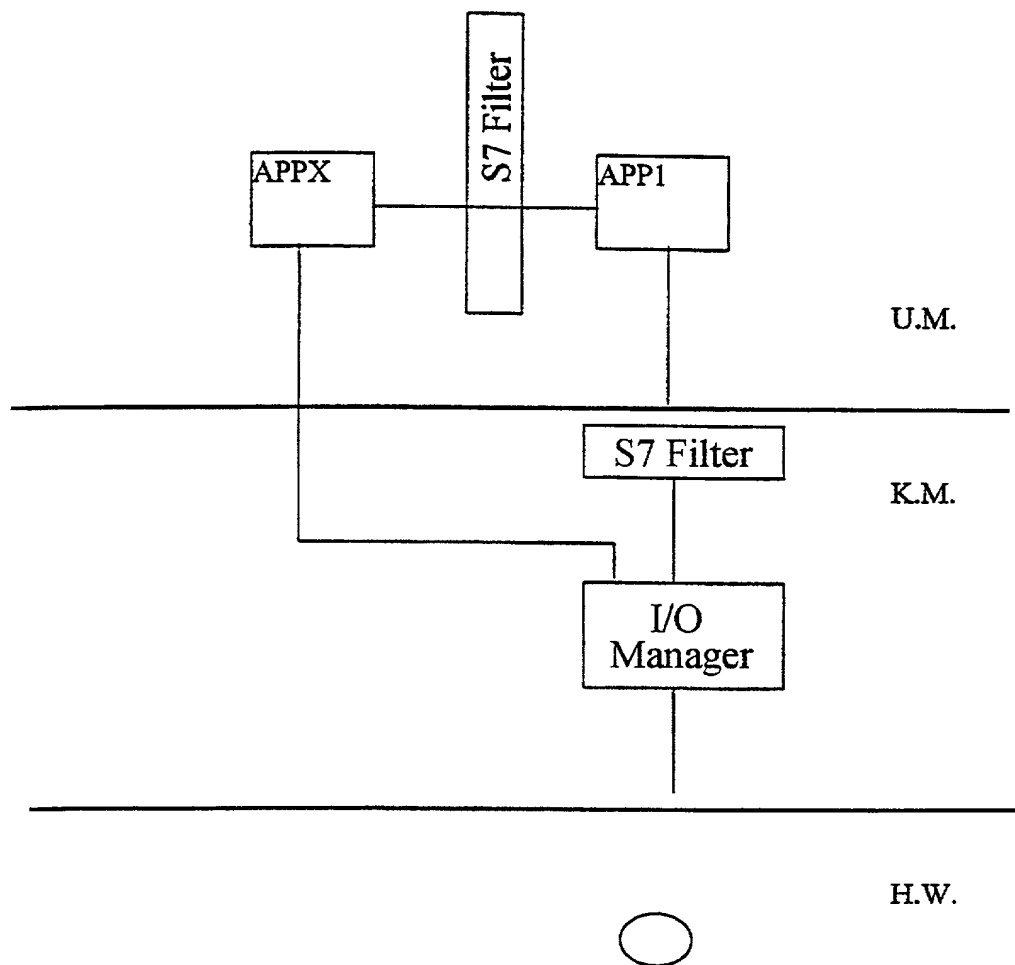
1/3

*Fig. 1*

2/3

*Fig. 2*

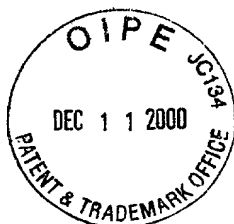
3/3

*Fig. 3*

20000055-PCT-US

09/622-9

11/23/2000



DECLARATION AND POWER OF ATTORNEY

As a below-named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND AGENT FOR THE PROTECTION AGAINST THE UNAUTHORIZED USE OF COMPUTER RESOURCES

(Title of Invention)

the specification of which:
(check one)

_____ is attached hereto.

X was filed on 25 February 1999

Application Serial No. PCT/IL99/00113

and was amended by _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Priority Claimed

<u>Number</u>	<u>Country</u>	<u>Filing Date</u>	<u>Yes</u>	<u>No</u>
<u>123512</u>	<u>Israel</u>	<u>March 2, 1998</u>	<u>X</u>	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

Declaration and Power of Attorney

Page 2

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States Application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

Application Serial No.Filing DateStatus

And I hereby appoint Ivan S. Kavrukov (Reg. No. 25161), Thomas F. Moran (Reg. No. 16579; Christopher C. Dunham (Reg. No. 22031); Norman H. Zivin (Reg. No. 25385), John P. White (Reg. No. 28678); Robert D. Katz (Reg. No. 30141); Peter J. Phillips (Reg. No. 29691); Richard S. Milner (Reg. No. 33970); Richard F. Jaworski (Reg. No. 33515); Raymond DiPerna (44063), and each of them, all c/o Cooper & Dunham LLP of 1185 Avenue of the Americas, New York, New York 10036 (Tel. 212-278-0400), my attorneys, each with full power of substitution and revocation, to prosecute this application, to make alterations and amendments therein, to receive the patent, to transact all business in the Patent and Trademark Office connected herewith and to file any International Applications which are based thereon under the provisions of the Patent Cooperation Treaty.

Please address all communications, and direct all telephone calls, regarding this application to:

Richard F. JaworskiReg. No. 33515Cooper & Dunham LLP1185 Avenue of the AmericasNew York, New York 10036Tel (212) 278-0400

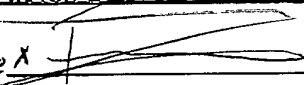
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or

first joint inventor Doron ELGRESSYInventor's signature XCitizenship IsraelDate of signature 24.10.2000Residence 31 Kish Street, 33531 Haifa, IsraelPost Office Address As above

631 342 4866

Full name of sole or

first joint inventor Fabian BEN ADERETInventor's signature Citizenship Israel

Date of signature

Nov 22, 2000Residence 6/2 Hashikma Street, Migdal Haemek 10500, IsraelPost Office Address As above.